



BLOCKONOMI

Fundamentals History

The History of the Mt Gox Hack: Bitcoin's Biggest Heist



Andrew Norry on November 29, 2017 / 1 Comment

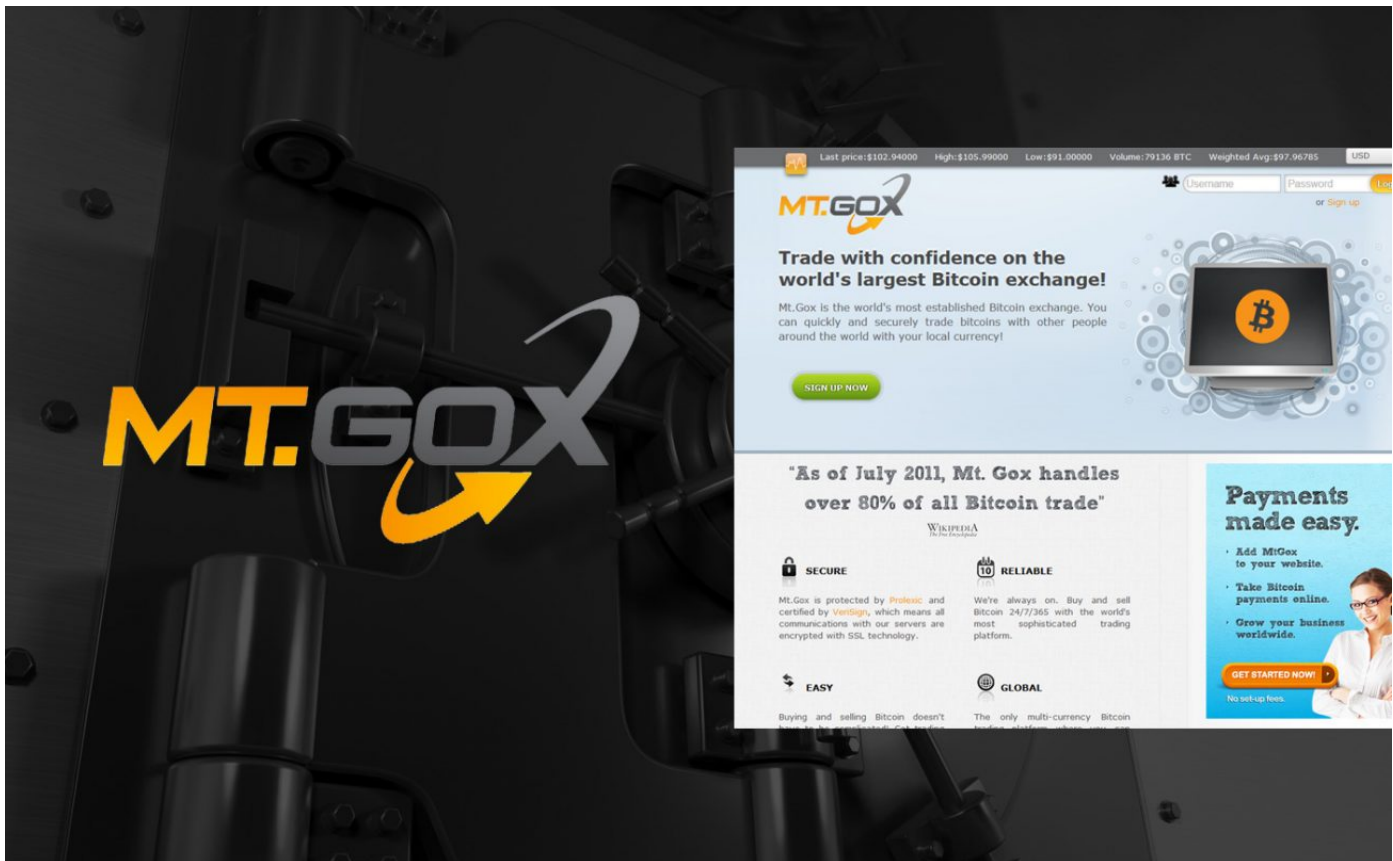
Post Views: 15,622

ICO Pre-sale
live now!**JOIN ICO PRESALE****97**
SHARESFacebook **81**Twitter **12**Google+ **2**LinkedIn **2**Buffer **0**

Subscribe

At the beginning of 2014, Mt Gox, a bitcoin exchange based in Japan, was the largest bitcoin exchange in the world, handling over 70% of all bitcoin transactions worldwide. By the end of February of that year, it was bankrupt.

The victim of a massive hack, Mt. Gox lost about 740,000 bitcoins (6% of all bitcoin in existence at the time), valued at the equivalent of €460 million at the time and over \$3 billion at October 2017 prices. An additional \$27 million was missing from the company's bank accounts. Although 200,000 bitcoins were eventually recovered, the remaining 650,000 have never been recovered.



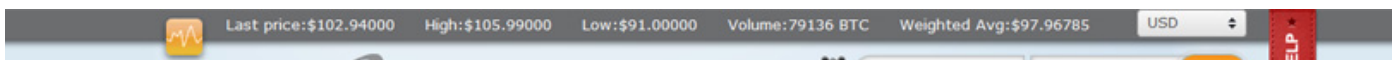
This post will discuss the rise and fall of Mt. Gox, the aftermath of the hack and the resulting (and ongoing) investigation and will consider whether it could happen again.

The Rise of the Mt Gox Exchange

Contents [\[show\]](#)

Launched in 2010 by US programmer Jed McCaleb (who later went on to found Ripple), Mt Gox expanded rapidly to become by far the most popular bitcoin exchange in the world after being purchased by French developer and bitcoin enthusiast Mark Karpelés in March 2011. Rather bizarrely the name Mt Gox stood for “Magic: The Gathering Online eXchange”.

In June 2011 the Mt. Gox exchange was hacked, most likely as a result of a compromised computer belonging to an auditor of the company. On that occasion, the hacker used their access to the exchange to artificially alter the nominal value of bitcoin to one cent and then transfer an estimated 2,000 bitcoins from customer accounts on the exchange, which were then sold. In addition, an estimated 650 bitcoins were purchased from the exchange at the artificially low price by Mt. Gox customers, none of which were ever returned. As a result of this hack Mt. Gox took a number of security measures, including arranging for a substantial amount of its bitcoin to be taken offline and held in cold storage.



MT.GOX

Trade with confidence on the world's largest Bitcoin exchange!

Mt.Gox is the world's most established Bitcoin exchange. You can quickly and securely trade bitcoins with other people around the world with your local currency!

SIGN UP NOW

"As of July 2011, Mt. Gox handles over 80% of all Bitcoin trade"

WIKIPEDIA
The Free Encyclopedia

SECURE
Mt.Gox is protected by Prolexic and certified by VeriSign, which means all communications with our servers are encrypted with SSL technology.

RELIABLE
We're always on. Buy and sell Bitcoin 24/7/365 with the world's most sophisticated trading platform.

EASY

GLOBAL

Payments made easy.

- Add MtGox to your website.
- Take Bitcoin payments online.
- Grow your business worldwide.

GET STARTED NOW!

In spite of the June 2011 hack, by 2013 Mt. Gox had established itself as the largest bitcoin exchange in the world, in part as a result of increased interest in bitcoin as the price of the coins increased rapidly (jumping from \$13 dollars in January 2013 to a peak of more than \$1,200).

However, behind the scenes all was not well.

The Struggles behind the scenes

Although Mt. Gox had quickly expanded to become the largest bitcoin exchange in the world by 2013, behind the scenes it was struggling. Since its collapse, a number of Mt. Gox employees have spoken about how Mt. Gox was operating, with a picture being painted of a disorganized and discordant organization, with poor security procedures, serious issues relating to the source code of the website and a number of serious issues arising in relation to the operation of the business.

In May 2013, a former business partner of Mt. Gox called Coinlab sued the company for \$75 million, claiming breach of contract. The two companies had signed an agreement under which Coinlab would take over Mt. Gox's American customers but, according to Coinlab's lawsuit, the deal failed to materialize due to Mt. Gox breaching a clause of the contract.

In addition, the US Department of Homeland Security was investigating claims that a subsidiary of Mt. Gox operating in the US was not licensed and was therefore operating as an unregistered money

transmitter. As a result of this investigation, more than \$5 million was seized by the US government from the company's bank accounts.

As a result of the US investigation, Mt. Gox had announced a temporarily suspension of withdrawals in US dollars. Although this suspension only nominally lasted for one month, many customers were experiencing delays of up to 3 months in withdrawing cash from their accounts and few US dollar withdrawals were being successfully completed. These delays resulted in Mt. Gox losing its place as the largest bitcoin exchange in the world by the end of 2013, falling to third.

However, as it turned out, these issues were the tip of the iceberg. Underneath the hood, Mt. Gox had much bigger problems than it realized. It had been the victim of an ongoing hacking for over two years.

The Mt. Gox hack

On 7 February 2014, Mt. Gox stopped all bitcoin withdrawals, claiming that it was merely pausing withdrawal requests "to obtain a clear technical view of the currency process." After a number of weeks of uncertainty, on 24 February 2014, the exchange suspended all trading and the website went offline. That same week, a leaked corporate document claimed that hackers had raided that Mt. Gox exchange and stole 744,408 bitcoins belonging to Mt. Gox customers, as well as an additional 100,000 bitcoins belonging to the company, resulting in the exchange being declared to be insolvent. On 28 February Mt. Gox filed for bankruptcy protection in Japan, and in the US two weeks later.

Subsequent investigations have shown that the massive hack of Mt. Gox had begun as early as September 2011. As a result, Mt. Gox was operating while technically insolvent for almost two years and had practically lost all of its bitcoins by mid-2013. Additional evidence has suggested that Mt. Gox was already missing up to 80,000 bitcoins from its exchange even before Mark Karpelés purchased the exchange in 2011.

Although it remains an ongoing investigation and the facts remain unclear at this time, it is presumed that most of the bitcoins that were stolen from Mt. Gox were taken from its online (or hot) wallets, including all of the currency being held in cold storage, due to a "leak" in the hot wallet. An online cryptocurrency wallet is a web-based wallet used to store secure digital codes, known as private keys that show ownership of a public digital code, known as a public key, that can be used to access the currency addresses and it is this information that is stored in a wallet. Prior to September 2011, the Mt. Gox private key was unencrypted and it would appear that it was stolen via a copied wallet.dat file, either by hacking or perhaps through an insider.

Once the file was hacked, the hacker(s) were able to access and cipher bitcoins gradually from the wallets associated with Mt. Gox's private keys without the hack being detected. The shared keypool of the copied file led to address re-use, which meant that the company appeared to be oblivious to the theft with the Mt. Gox systems interpreting the transfers as deposits apparently being moved to more

there, with the Mt. Gox system interpreting the transfers as deposits apparently being moved to more secure addresses. Whenever the wallets emptied, the Mt Gox system's interpretation of the theft as deposits resulted in an additional 40,000 extra bitcoins being credited to multiple user accounts.

The Aftermath

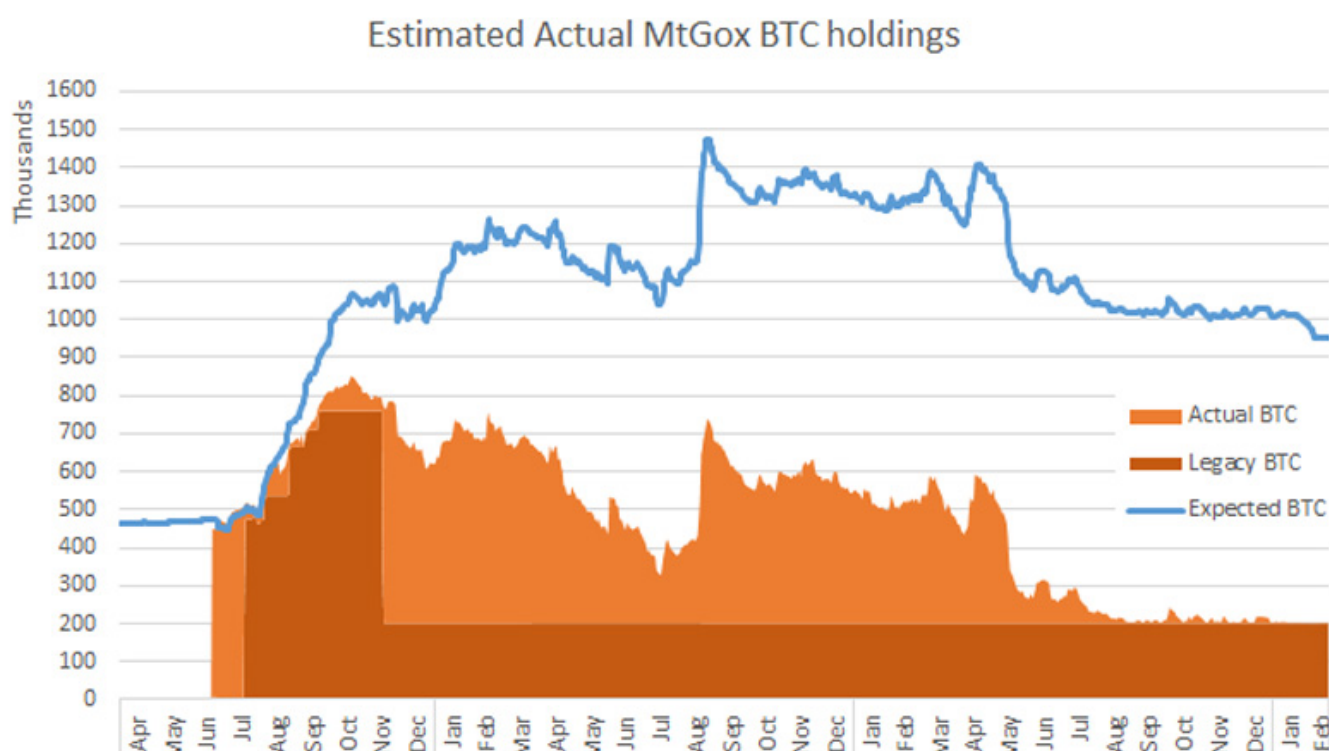
In March 2014, Mt. Gox reported on its website that it had found 200,000 bitcoins in old-format digital wallets that had been used by the exchange prior to June 2011. These bitcoins remain held on trust for creditors while the company remains under bankruptcy protection.

Mark Karpelés was arrested in Japan in August 2015 and charged with fraud and embezzlement, although none of these charges directly relate to the theft. He was imprisoned until July 2016, when he was released on bail. He has pleaded not guilty to the charges and his trial is ongoing.

Mt. Gox remains under bankruptcy protection, with the case still being under investigation. In addition, the litigation with CoinLab remains outstanding and distribution to creditors cannot occur until that lawsuit is settled.

Where did the money go?

650,000 bitcoins remain unaccounted for as a result of the Mt. Gox hack. A number of online theories have been developed as to where the missing coins are. Some have suggested that Mt. Gox never had the amount of coins that it claimed, and that Karpelés had manipulated the numbers to make it appear that Mt. Gox held more bitcoin than it in fact held.



2011	2012	2013	2014
------	------	------	------

In respect of how the hacker was able to access the bitcoins that Mt. Gox held in cold storage, the theories range from suggestions that the storage may have been compromised by an individual with on-site access to suggestions that the cold storage coins were gradually deposited into the Mt. Gox exchange system when a hot wallet ran low, and that a lack of accountability among staff simply meant that there was no awareness that the wallets were being drained by hackers.

In July 2017, a Russian national named Alexander Vinnik was arrested by US authorities in Greece and charged with playing a key role in the laundering of bitcoins stolen from Mt. Gox. In addition Vinnik was charged by Greek authorities for laundering of approximately \$4 billion in bitcoin. Vinnik is alleged to be associated with BTC-e, a well-established bitcoin exchange, which was raided by the FBI as part of the investigation. The BTC-e site has been shut down and the domain has been seized by the FBI, the first time the US government has seized a foreign exchange on foreign soil. Investigations by Wizsec, a group of bitcoin security specialists, had identified Vinnik as the owner of the wallets into which the stolen bitcoins had been transferred, many of which were sold on BTC-e.



With the trial of Mark Karpelés ongoing in Japan and the indictment against Vinnik, it would appear that the separate strands of the investigation into the Mt. Gox hack are finally coming together. Whether any

OR THIS WILL RESULT IN THE RECOVERY OF ALL OR ANY OF THE STOLEN BITCOINS REMAINS TO BE SEEN, BUT IT DOES APPEAR THAT WE WILL HAVE AT LEAST SOME CLARITY INTO THE MT. GOX HACK IN THE NEAR FUTURE.

Could it happen again?

The short answer is that it could. There are many bitcoin exchanges operating at present, some of which are more reputable than others. [Popular exchanges](#) such as [Coinbase](#) are relatively transparent about their operations, as well as offering insured deposits, and are backed by reputable venture capitalists. However, they are also going to be the targets of the best hackers, who will be only too happy to exploit any security gaps.

In addition, there are many smaller exchanges currently trading that aren't as clear about how they operate. That does not mean that such exchanges are operating a hack or disreputable in any way. But when it comes to [cryptocurrency](#) trading, it is recommended that you use the more reputable exchanges, if only for your own peace of mind, unless you have the means to absolutely guarantee the legitimacy of any smaller exchange that you are dealing with.

And if the above isn't enough to scare you, my one last word of advice would be to make sure that you don't store your bitcoins on any exchange. See our post on [cryptocurrency wallets](#) for more details on how to store your bitcoins.

97
SHARES



Facebook **81**



Twitter **12**



Google+ **2**



LinkedIn **2**



Buffer **0**



Subscribe



Blockonomi Updates ...

Receive our Latest Guides & ICO News

Join our mailing list and be the first to receive our beginners guides, mining tutorials and ICO news.

[Sign Up](#)

Posted in: Fundamentals, History

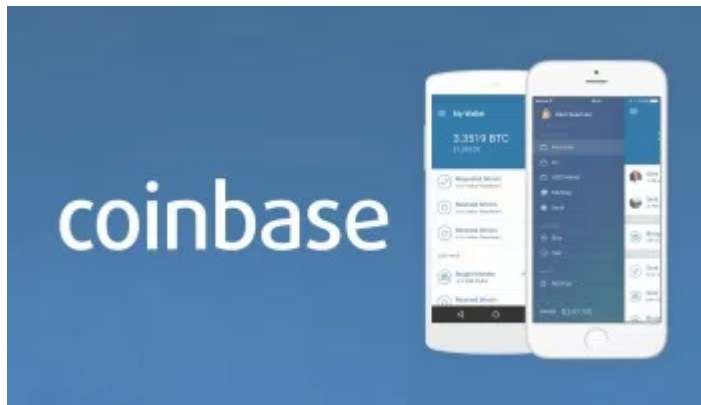
Tagged in: mt gox exchange, mt gox hack, mt gox history, The History of the Mt Gox Hack



Posted by Andrew Norry

[All Posts](#)

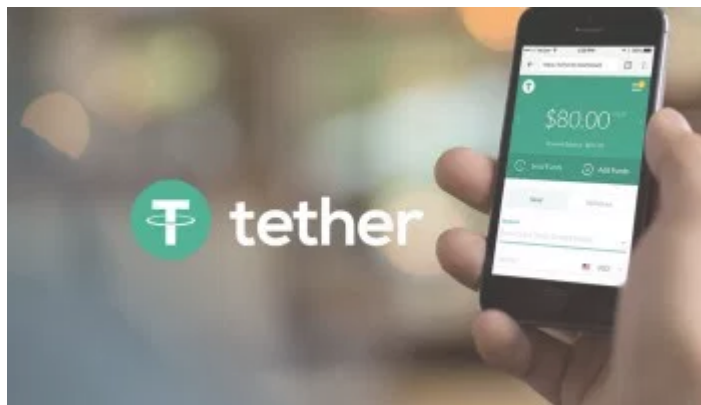
Related:



Beginner's Guide to Coinbase: Complete Review

November 13, 2017

In "Exchanges"



Beginner's Guide to Tether

January 3, 2018

In "Guides"



What Are Atomic Swaps? Our Guide to a Revolution in Decentralization

January 10, 2018

In "Fundamentals"

All content on Blockonomi.com is provided solely for informational purposes, and is not an offer to buy or sell or a solicitation of an offer to buy or sell any security, product, service or investment. The opinions expressed in this Site do not constitute investment advice and independent financial advice should be sought where appropriate.

One Comment

**Dan**

MARCH 5, 2018 AT 10:18 AM

Do you need help recovering lost bitcoins? Contact: INCFIDELIBUS at GMAIL dot COM

Reply

Leave a reply

Comment

Name ***Email *****Website**

Post Comment

☐

Notify me of follow-up comments by email.

☐

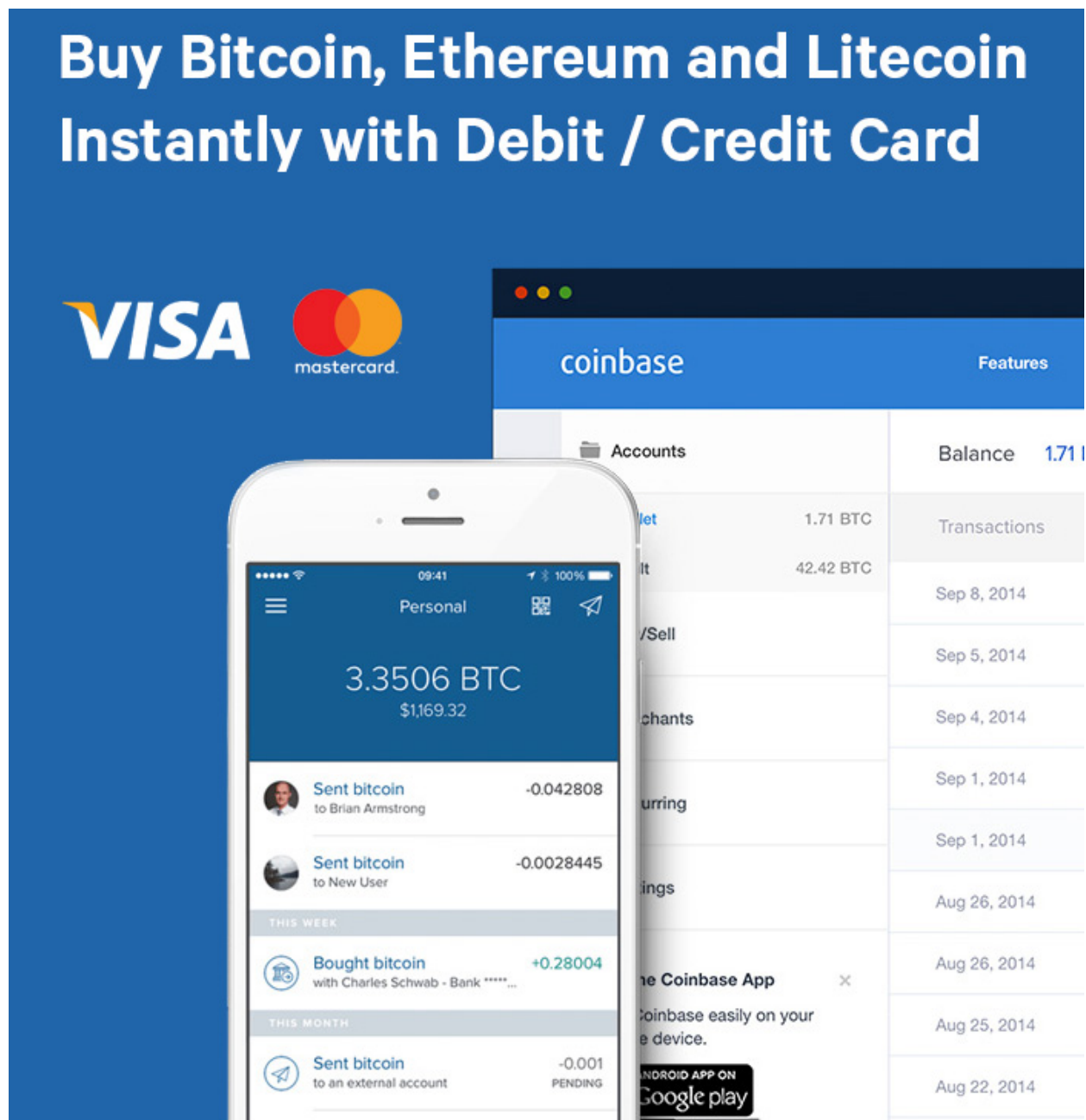
Notify me of new posts by email.



Coinbase

The Coinbase logo, featuring the word "coinbase" in white lowercase letters on a solid blue rectangular background.

Buy Bitcoin, Ethereum and Litecoin Instantly with Debit / Credit Card



The image is a promotional graphic for Coinbase. At the top, a blue banner contains the text "Buy Bitcoin, Ethereum and Litecoin Instantly with Debit / Credit Card" in white. Below the banner, on the left, are the Visa and Mastercard logos. In the center, a white smartphone displays the Coinbase mobile app interface, showing a balance of 3.3506 BTC (\$1,169.32) and a list of transactions. To the right, a desktop screen displays the Coinbase website interface, showing a balance of 1.71 BTC and a list of transactions. The desktop screen also features a "Features" link and a "Coinbase App" download button.

Accounts	Balance
1.71 BTC	1.71
42.42 BTC	42.42

Transactions
Sep 8, 2014
Sep 5, 2014
Sep 4, 2014
Sep 1, 2014
Sep 1, 2014
Aug 26, 2014
Aug 26, 2014
Aug 25, 2014
Aug 22, 2014

Buy Bitcoin & Ethereum Instantly Online

Let's Connect

Follow us on social media & join our growing audience who get the latest ICOs, Crypto Reviews and Guides from Blockonomi.



Categories

Buying

Exchanges

Fundamentals

Guides

History

ICO

Mining

Press Release

Wallets

Crypto Guides

Best Cryptocurrency Exchanges for Beginners

Best Bitcoin Wallets 2018

Best Ethereum Wallets 2018

Trezor vs Ledger Review

How to Buy Ethereum using a Credit or Debit Card

How to Buy Bitcoin using a Credit or Debit Card

How to Buy Bitcoin With PayPal

Binance Review

Kucoin Review

Coinbase Review

Localbitcoins Review

IQ Option Review

Protect Your Cryptos

Ledger Nano S

The most recommended
cryptocurrency hardware wallet



58€

+ V.A.T.
where applicable

BUY NOW

Protect your Cryptos with a Hardware Wallet

Next

Best Bitcoin Wallets 2018: Hardware vs Software vs Paper

September 28, 2017

Previous

The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin

October 11, 2017



Blockonomi™ Copyright © 2017 - 2018 Kooc Media Ltd. All rights reserved. Registered Company No.05695741

Cryptocurrencies, Technology and the Blockchain Economy.

[Terms & Conditions](#) / [Privacy Policy](#).